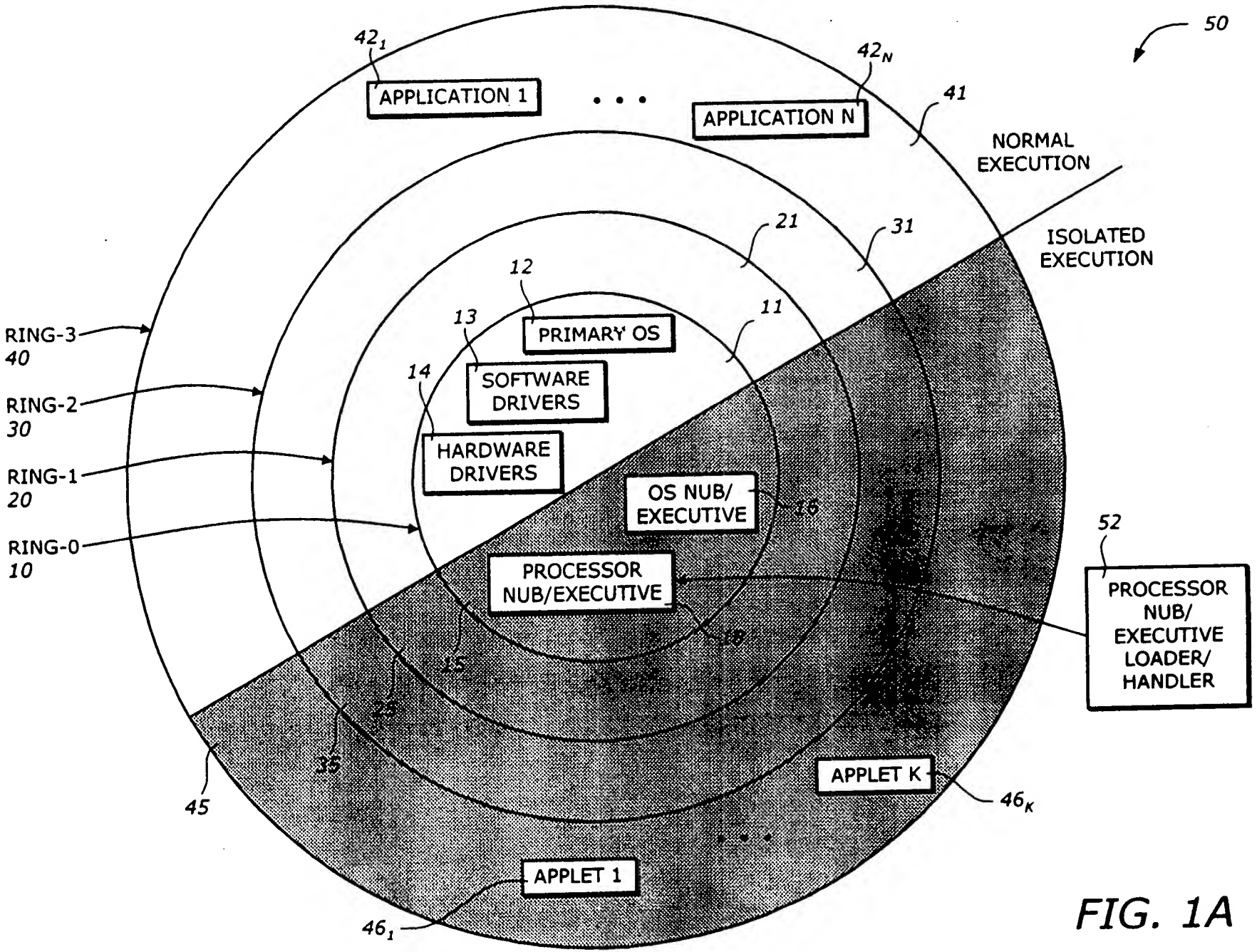
50
42₁
APPLICATION 1
42N
APPLICATION N
41
NORMAL EXECUTION
ISOLATED EXECUTION
21
31
12
PRIMARY OS
13
SOFTWARE DRIVERS
14
HARDWARE DRIVERS
11
RING-3
40
RING-2
30
RING-1
20
RING-0
10
OS NUB/ EXECUTIVE
16
PROCESSOR NUB/EXECUTIVE
18
52
PROCESSOR NUB/ EXECUTIVE LOADER/ HANDLER
15
25
35
45
APPLET K
46K
APPLET 1
46₁

FIG. 1A

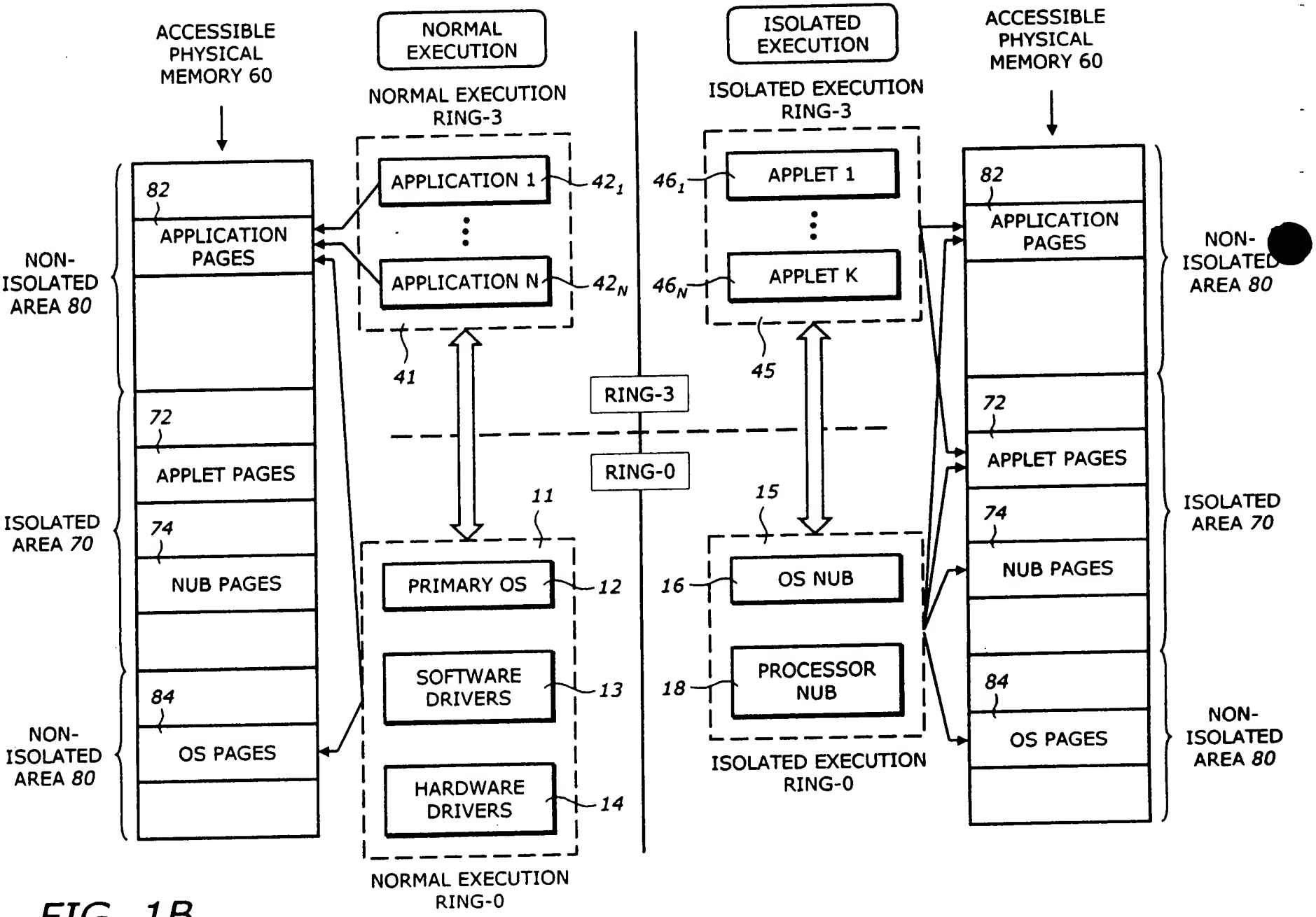
ACCESSIBLE PHYSICAL MEMORY 60
NORMAL EXECUTION
ISOLATED EXECUTION
ACCESSIBLE PHYSICAL MEMORY 60
NORMAL EXECUTION RING-3
ISOLATED EXECUTION RING-3
82
APPLICATION PAGES
APPLICATION 1
42$_1$
APPLICATION N
42$_N$
46$_1$
APPLET 1
46$_N$
APPLET K
NON-ISOLATED AREA 80
41
45
RING-3
RING-0
72
APPLET PAGES
74
NUB PAGES
ISOLATED AREA 70
11
15
PRIMARY OS
12
SOFTWARE DRIVERS
13
HARDWARE DRIVERS
14
16
OS NUB
18
PROCESSOR NUB
84
OS PAGES
NON-ISOLATED AREA 80
NORMAL EXECUTION RING-0
ISOLATED EXECUTION RING-0

FIG. 1B

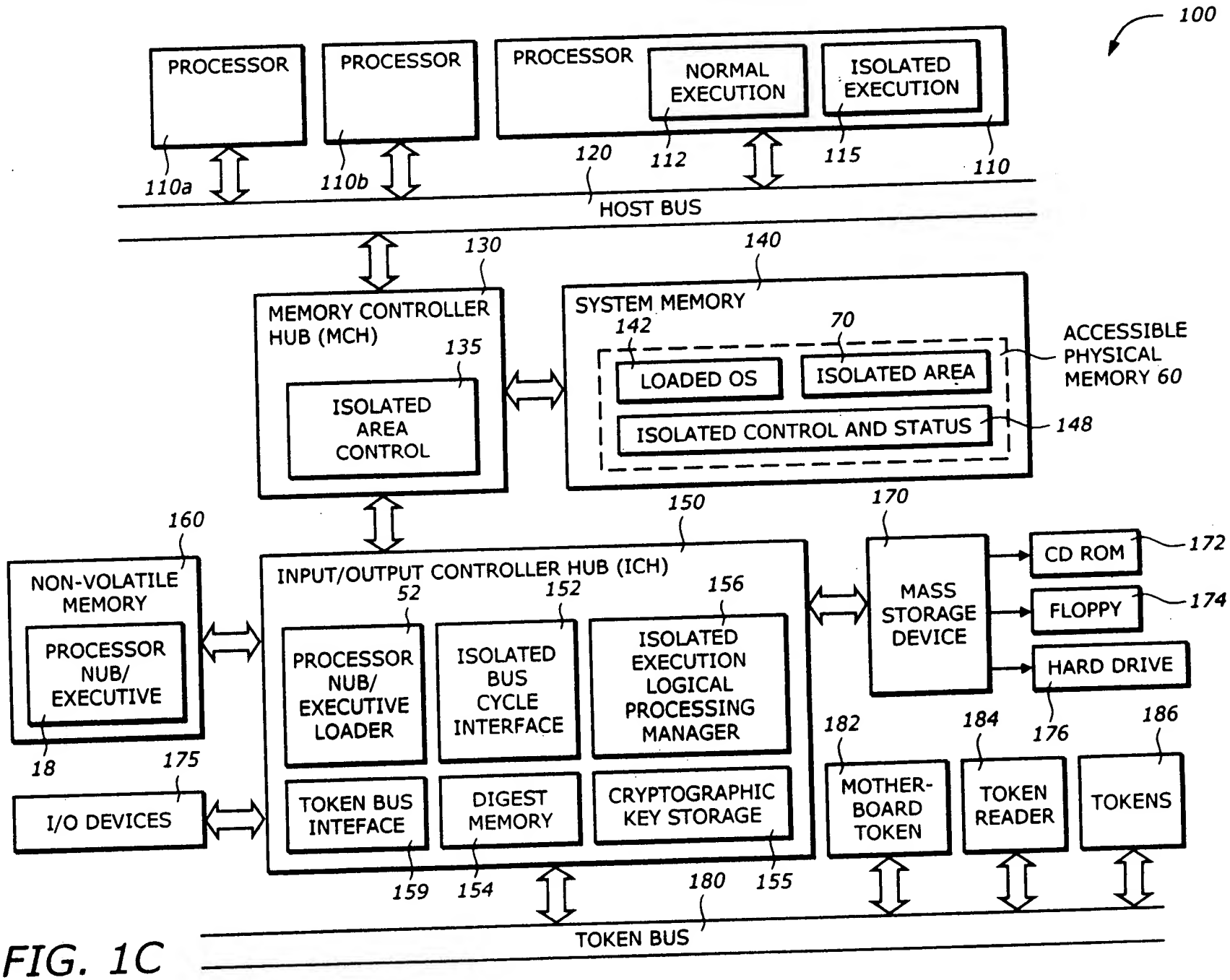
100
PROCESSOR
PROCESSOR
PROCESSOR
NORMAL EXECUTION
ISOLATED EXECUTION
110a
110b
120
112
115
110
HOST BUS
130
140
MEMORY CONTROLLER HUB (MCH)
135
ISOLATED AREA CONTROL
SYSTEM MEMORY
142
70
LOADED OS
ISOLATED AREA
ISOLATED CONTROL AND STATUS
148
ACCESSIBLE PHYSICAL MEMORY 60
160
150
170
NON-VOLATILE MEMORY
PROCESSOR NUB/ EXECUTIVE
INPUT/OUTPUT CONTROLLER HUB (ICH)
52
152
156
PROCESSOR NUB/ EXECUTIVE LOADER
ISOLATED BUS CYCLE INTERFACE
ISOLATED EXECUTION LOGICAL PROCESSING MANAGER
MASS STORAGE DEVICE
CD ROM
172
FLOPPY
174
HARD DRIVE
18
175
176
182
184
186
I/O DEVICES
TOKEN BUS INTEFACE
DIGEST MEMORY
CRYPTOGRAPHIC KEY STORAGE
MOTHER-BOARD TOKEN
TOKEN READER
TOKENS
159
154
180
155
TOKEN BUS

FIG. 1C

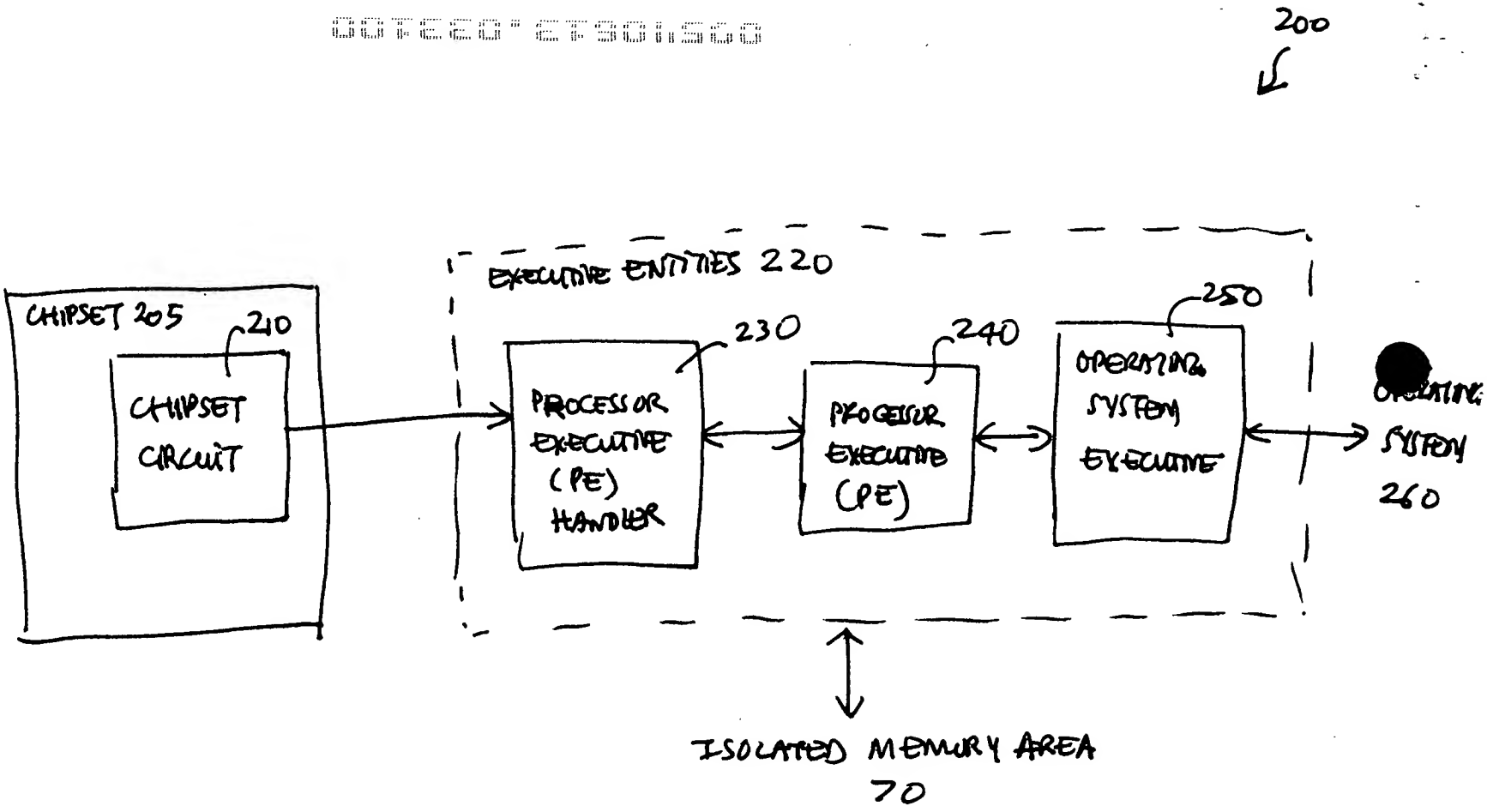

FIG. 2

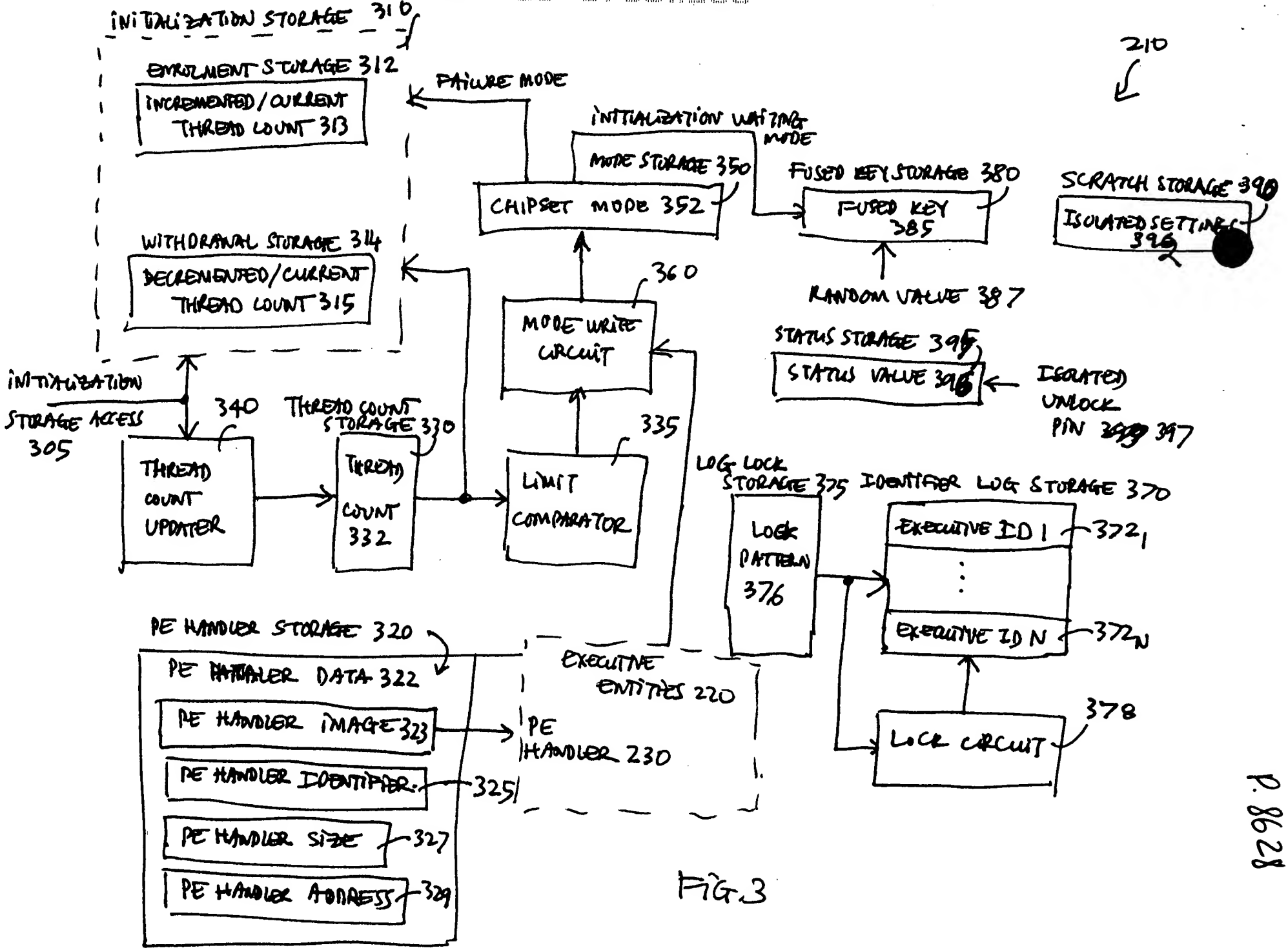
INITIALIZATION STORAGE 310
ENROLLMENT STORAGE 312
INCREMENTED/CURRENT THREAD COUNT 313
WITHDRAWAL STORAGE 314
DECREMENTED/CURRENT THREAD COUNT 315
INITIALIZATION STORAGE ACCESS 305
340
THREAD COUNT UPDATER
THREAD COUNT STORAGE 330
THREAD COUNT 332
335
LIMIT COMPARATOR
360
MODE WRITE CIRCUIT
FAILURE MODE
INITIALIZATION WAITING MODE
MODE STORAGE 350
CHIPSET MODE 352
FUSED KEY STORAGE 380
FUSED KEY 385
RANDOM VALUE 387
SCRATCH STORAGE 390
ISOLATED SETTING 392
STATUS STORAGE 395
STATUS VALUE 396
ISOLATED UNLOCK PIN 397
LOG LOCK STORAGE 375
LOCK PATTERN 376
IDENTIFIER LOG STORAGE 370
EXECUTIVE ID 1 372 1
EXECUTIVE ID N 372 N
LOCK CIRCUIT 378
PE HANDLER STORAGE 320
PE HANDLER DATA 322
PE HANDLER IMAGE 323
PE HANDLER IDENTIFIER 325
PE HANDLER SIZE 327
PE HANDLER ADDRESS 329
PE HANDLER 230
EXECUTIVE ENTITIES 220
210

FIG. 3

P. 8628

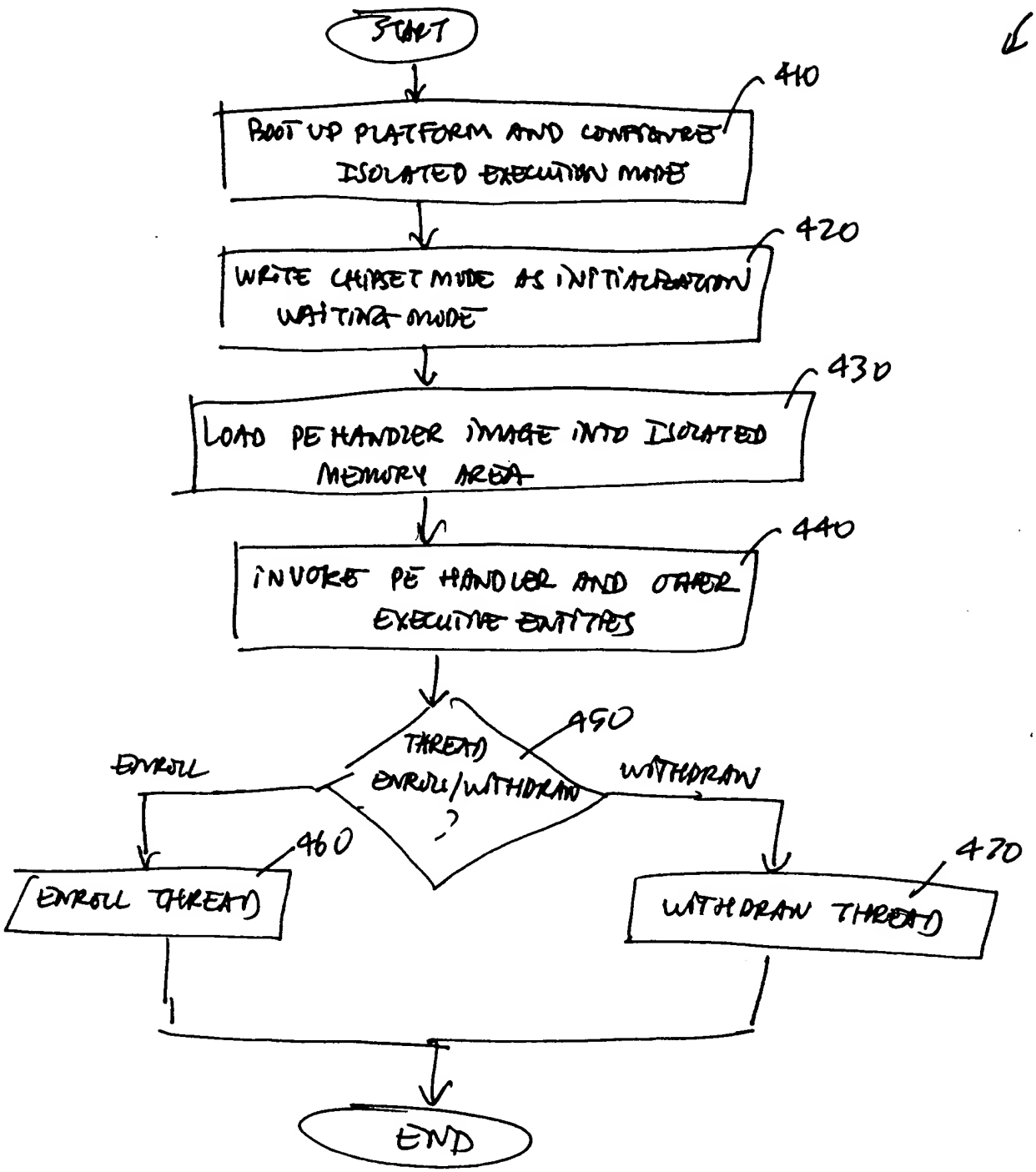
400
START
410
BOOT UP PLATFORM AND CONFIGURE ISOLATED EXECUTION MODE
420
WRITE CHIPSET MODE AS INITIALIZATION WAITING MODE
430
LOAD PE HANDLER IMAGE INTO ISOLATED MEMORY AREA
440
INVOKE PE HANDLER AND OTHER EXECUTIVE ENTITIES
450
THREAD ENROLL/WITHDRAW ?
ENROLL
WITHDRAW
460
ENROLL THREAD
470
WITHDRAW THREAD
END

FIG 4

460

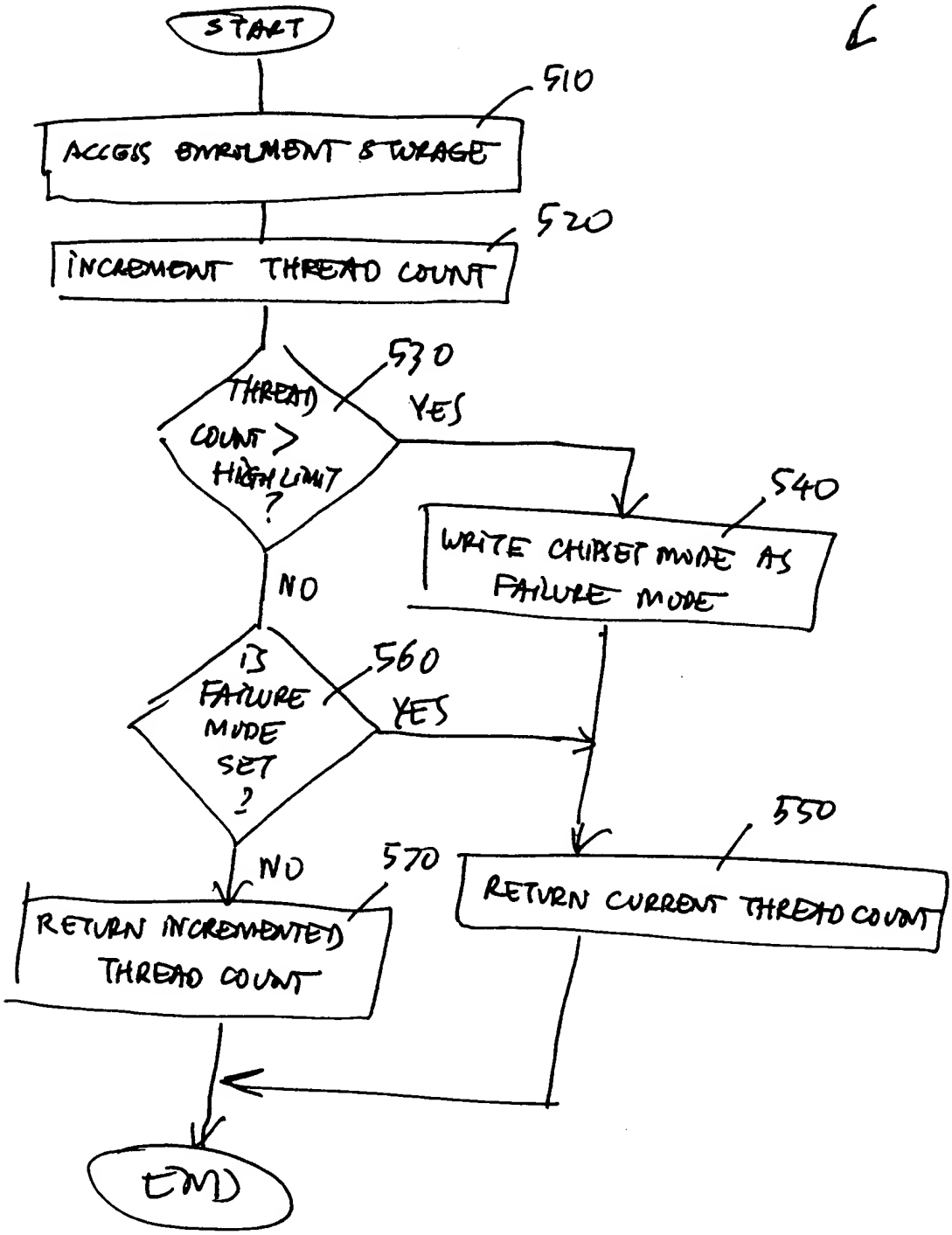
START
510
ACCESS ENVIRONMENT STORAGE
520
INCREMENT THREAD COUNT
530
THREAD COUNT > HIGH LIMIT ?
YES
NO
540
WRITE CHIPSET MODE AS FAILURE MODE
560
IS FAILURE MODE SET ?
YES
NO
570
RETURN INCREMENTED THREAD COUNT
550
RETURN CURRENT THREAD COUNT
END

FIG. 5

470

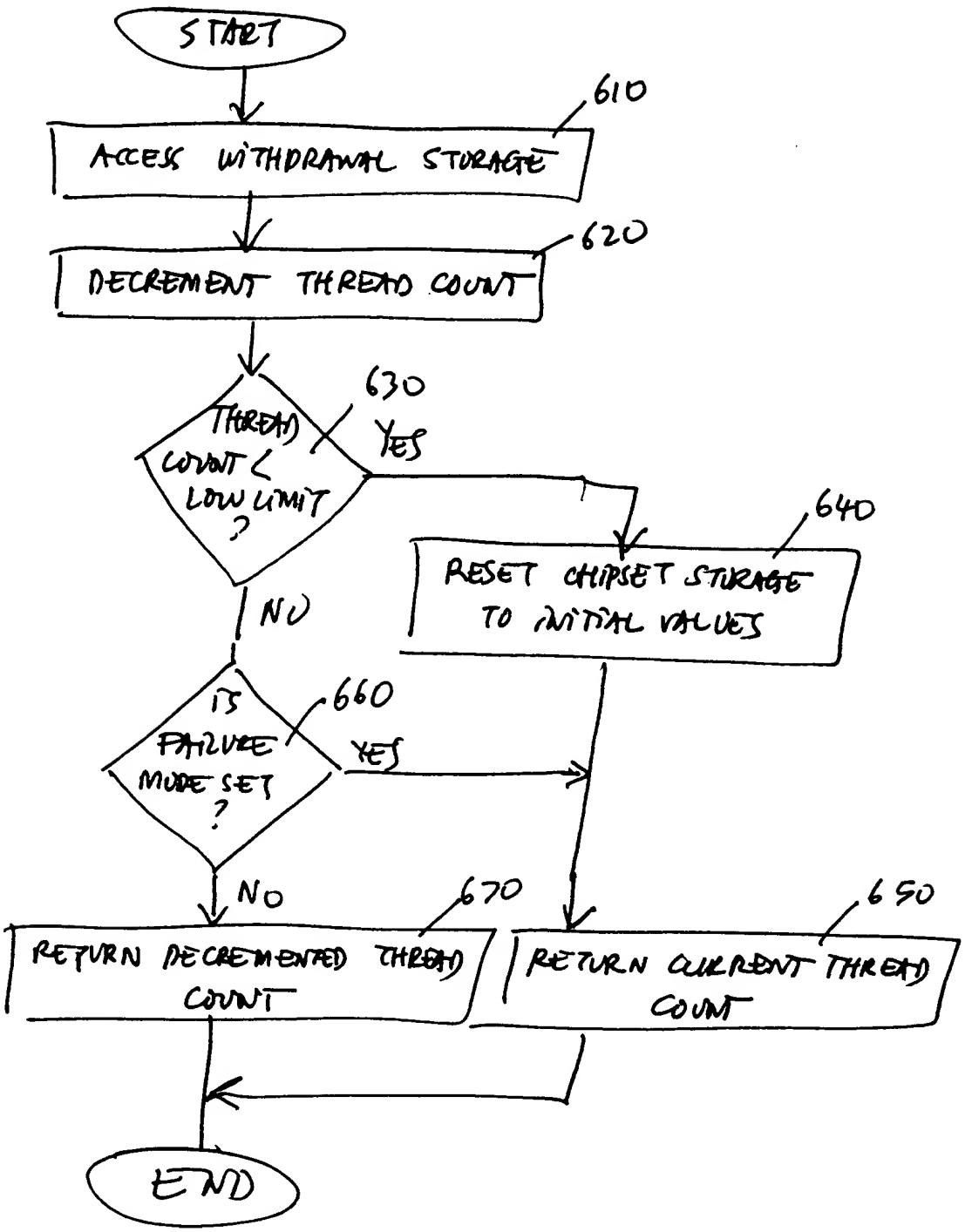
START
610
ACCESS WITHDRAWAL STORAGE
620
DECREMENT THREAD COUNT
630
THREAD COUNT < LOW LIMIT ?
YES
NO
640
RESET CHIPSET STORAGE TO INITIAL VALUES
660
IS FAILURE MODE SET ?
YES
NO
670
RETURN DECREMENTED THREAD COUNT
650
RETURN CURRENT THREAD COUNT
END

FIG. 6

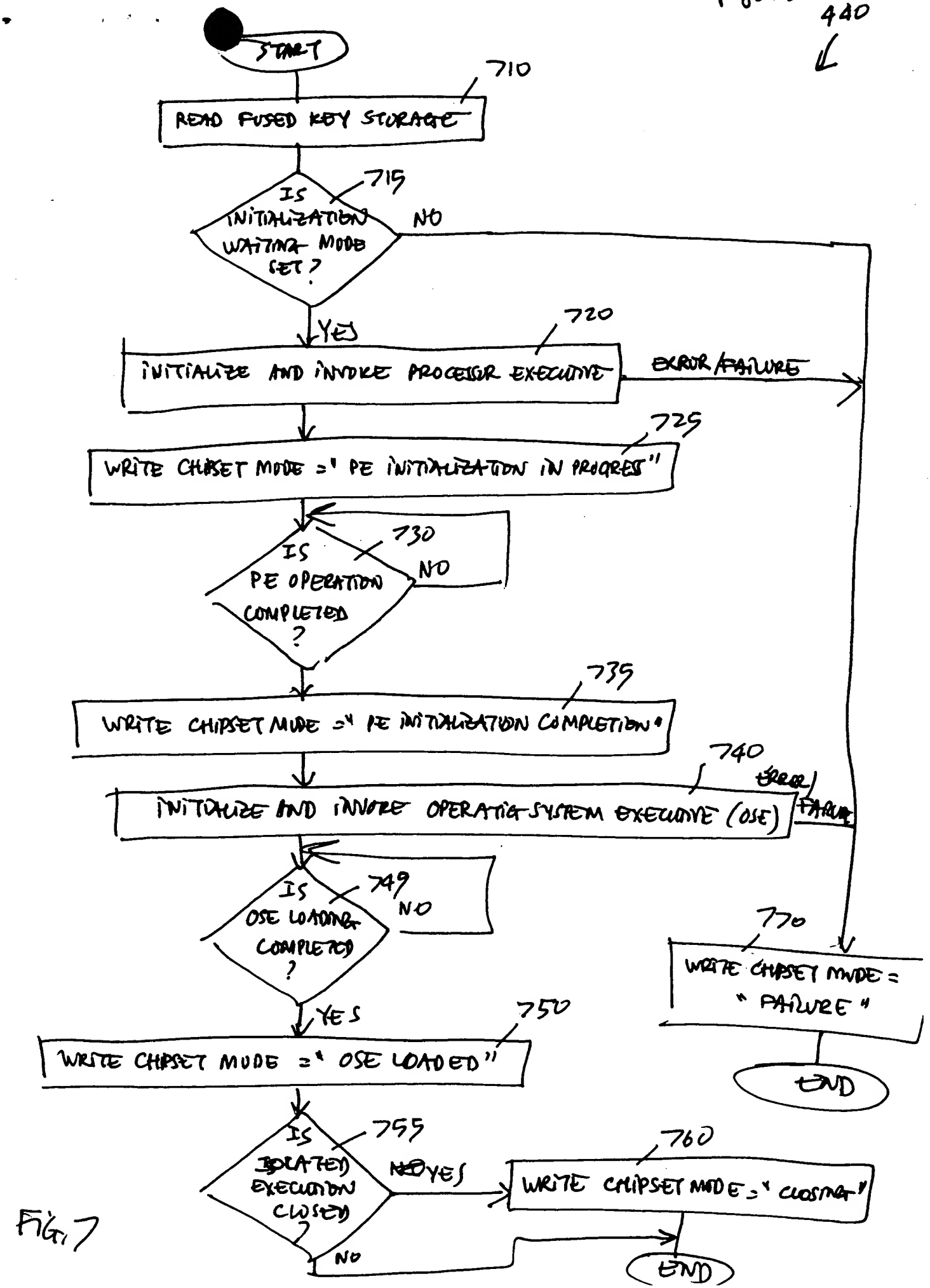
440
START
710
READ FUSED KEY STORAGE
715
IS INITIALIZATION WAITING MODE SET?
NO
YES
720
INITIALIZE AND INVOKE PROCESSOR EXECUTIVE
ERROR/FAILURE
725
WRITE CHIPSET MODE = "PE INITIALIZATION IN PROGRESS"
730
IS PE OPERATION COMPLETED?
NO
735
WRITE CHIPSET MODE = "PE INITIALIZATION COMPLETION"
740
INITIALIZE AND INVOKE OPERATING SYSTEM EXECUTIVE (OSE)
ERROR/FAILURE
745
IS OSE LOADING COMPLETED?
NO
YES
750
WRITE CHIPSET MODE = "OSE LOADED"
755
IS ISOLATED EXECUTION CLOSED?
NO
YES
760
WRITE CHIPSET MODE = "CLOSING"
770
WRITE CHIPSET MODE = "FAILURE"
END
END

FIG. 7